REMARKS/ARGUMENTS

The Office Action has been carefully considered. Claims 1-33 are pending. Claims 34-42 are withdrawn. Claims 1-33 were rejected in the following manner:

1. Claims 25-26 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,775,779 to England et al. ("*England*").
2. Claims 27-28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *England*.
3. Claims 1-24 and 29-33 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *England*, in view of U.S. Patent No. 5,991,399 to Graunke ("*Graunke*").

35 U.S.C. § 102 Rejections

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP § 2131 (quoting *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)).

Claims 25-26 were rejected under 35 U.S.C. §102(e) as being anticipated by *England*. Applicants respectfully submit that Claims 25-26 are allowable at least because *England* does not disclose several elements of Claims 25-26, as discussed in detail below.

Claim 25 recites as follows:

A processor implemented method comprising;

verifying with a root one of a plurality of hierarchically organized digital content rendering modules, that each module that occupies an immediate downstream position in the hierarchy of modules from the root module has not been compromised, during an initialization period;

exclusively receiving with the root one of the plurality of hierarchically organized digital content rendering modules a first digital content of a first type;

rendering in part with said root one of said modules said first digital content;

re-verifying with said root one of said modules that one of the at least one other one of the modules occupying an immediate downstream position in the hierarchy of modules from the root module is uncompromised; and

transferring with said root one of said modules the first digital content to the re-verified immediate downstream module to further the rendering of the first digital content.

England is summarized as follows: "Secure pages handle premium content with a system of code modules in a hierarchy of trust, where a module names other modules that it is willing to trust, and those modules in turn name other modules that they are willing to trust." Col. 3 lines 14-17. The operation of hierarchical trust during operation is illustrated at blocks 540 in Fig. 5. In pertinent part, *England* describes its operation, at col. 14 lines 37-50, as follows:

> A normal, untrusted module... executes in block 541. If that module calls a trusted module, block 542 starts trusted interrupt handler 422.... If the security manager names the called module as trusted, block 543 causes block 544 to verify that its signature is correct.... Block 545 sets the secure-page permissions for that trusted module in the access-control table. Block 546 then executes the module. This module can in turn call another trusted module, which performs blocks 543-546 for the called module, using the names and signatures in the calling module to determine trust in this next level, and so on for any number of levels of a trust hierarchy.

Applicants respectfully submit that *England* does not disclose at least the following elements of Claim 25: "**rendering in part**... said first digital content; **re-verifying**... that one of the [immediate downstream modules] is uncompromised; and transferring... the first digital content to the **re-verified immediate downstream module** to further the rendering of the first digital content." Indeed, as set out in the passage from col. 14, above, *England* at best discloses merely a single verification step, "block 544 [verifies] that its signature is correct...." *England* never discloses that a root digital content rendering module verifies downstream modules, **partially renders** a digital content, **re-verifies** a downstream module, and transfers the partly rendered digital content to the re-verified downstream module for further rendering, as claimed in Claim 25.

None of the passages cited in the Office Action disclose these steps. Col. 8 lines 25-35 are directed towards merely identifying trustworthy modules, not verifying and also re-verifying modules, as claimed in Claim 25. Col. 11 lines 6-31 are directed towards merely providing cryptographic services by a security manager, not a digital content rendering module, for identifying, not verifying, a trusted module, not a digital content rendering module. No other passages from *England* are cited against Claim 25, and Applicants have been unable to discern any other passages that could be said to anticipate any of the above-discussed elements of Claim 25.

Accordingly, Applicants respectfully submit that Claim 25 is allowable over *England* for at least the reasons just discussed. Claim 26 depends from Claim 25 and is allowable at least by dependency.

35 U.S.C. § 103 Rejections

To establish a *prima facie* case of obviousness, Office personnel have the burden to meet three basic criteria. First, Office personnel must show that there is some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine the reference teachings. The teaching or suggestion to make the claimed combination must be found in the prior art, not based on applicant's disclosure. Second, Office personnel must show that the teachings in the prior art have a reasonable expectation of success. Finally, Office personnel must show that the combined prior art references teach or suggest all the claim limitations. *See* MPEP § 2142.

***England* does not teach or suggest every element of Claims 27-28.**

Claims 27-28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *England*. As characterized in the Office Action, Claim 27 is similar to Claim 25, but with the addition of a second operation on a second protected digital content of the first type. Similarly, as characterized in the Office Action, Claim 28 is similar to Claim 25, but with the addition of a second operation on a second protected digital content of a second type. For at least the reasons set out above, Applicants respectfully submit that *England* does not teach or even suggest that a root digital content rendering module verifies downstream modules, **partially renders** a first digital content, **re-verifies** a downstream module, and transfers the partly rendered first digital content to the re-verified downstream module for further rendering, let alone that a root module performs a second, similar operation on a second digital content. Accordingly, Applicants respectfully submit that Claims 27-28 are in condition for allowance.

***England* in view of *Graunke* does not teach or suggest every element of Claims 1-24 and 29-33.**

Claims 1-24 and 29-33 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *England* in view of *Graunke*. For at least the reasons discussed below, Applicants respectfully disagree.

Claim 1 recites as follows:

An apparatus comprising:

a tamper resistant digital content recovery module to recover protected digital contents of various types, the recovery module employing measures to hinder observation of operations performed therein;

a plurality of **plain text digital content rendering modules** communicatively coupled with each other in a hierarchical manner forming a hierarchy of modules, with selective combinations of the **plain text digital content rendering modules** to be selectively employed to render the recovered digital contents of the various types, including one of the **plain text digital content rendering modules** occupying a root position of the hierarchy to exclusively receive all types of the recovered digital contents to be rendered, from the tamper resistant digital content recovery module;

one or more storage units operative to store said tamper resistant module and said plurality of plain text digital content rendering modules; and

a processor coupled with the one or more storage units to execute the tamper resistant module and the plurality of plain text digital content rendering modules.

In the specification at ¶ [24], the term "plain text" (aka plaintext) is defined: "modules 102 may be provided and operated in plaintext (i.e. in an **unprotected** state)." Thus, plain text means unprotected or not secured. This definition is entirely in keeping with the ordinary definition of the term, as would be understood by one of ordinary skill in the art.

In the Office Action, *England* is said to teach "selective combinations of the **plain text digital content rendering modules** to be selectively employed to render the recovered digital contents of the various types." However, Applicants respectfully submit that *England* in view of *Graunke* discloses only secure or protected digital content rendering modules. For example, in one passage cited in the Office Action, Col. 8 lines 25-34, *England* discloses as follows: "The **secure content-provider module** 441, receiving trust from security manager 420, in turn entrusts a further, lower level of trust in other modules. .... Each **secure module** can contain names of one or more other specific modules it is willing to trust, and can confer trust upon them when it receives trust from higher in the tree." Similarly, at col. 10 lines 3-58, *England* states, "Normal OS mechanisms reschedule security manager 420, which in turn reschedules the secure module. The security manager is responsible for setting up an address space in protected memory appropriate for a secure module that is about to run." At col. 13 lines 27-33, "A secure module is able to confer trust upon a device plugged into a particular slot. .... [A] secure module can verify this identity and grant read access for a specific region

of memory to a particular hardware peripheral device." At col. 7 lines 66-67, "The root of trust of secure code modules is a secure loader 410…." Discussing "Secure DLL," item 441 in Fig. 4, at col. 8 lines 15-20, *England* clearly indicates that the secure dll is protected or non-plain text: "only one dynamic link library (DLL) 441 used by application 440 requires trust in order to protect the content. [It] is likely that a **single secure DLL** can provide protection for other applications as well."

In *England*, Fig. 4 includes "other non-secure modules," presumably such as those marked simply "DLL." However, in contrast to Claim 1, these non-secure DLLs serve no part in rendering protected digital content. Similarly, at col. 14 lines 1-2, *England* discloses that in some circumstances, "manager 420 can be stored in a non-encrypted cleartext form." However, in contrast to Claim 1, "manager 420" is not a digital content rendering module. Rather, *England's* components that may participate directly in rendering content exist several levels below manager 420. *See, e.g.,* col. 8 lines 25-30.

Thus, *England* never teaches or even suggests "selective combinations of the **plain text digital content rendering modules** to be selectively employed to render the recovered digital contents of the various types," as claimed in Claim 1. Applicants can discern no teaching or suggestion in *Graunke* that would remedy this defect. Accordingly, Applicants respectfully submit that for at least the reasons just discussed, Claim 1 is not obvious considering *England* in view of *Graunke*. Claims 2-17 and 29-33 also recite, either directly or by dependency, a similar plain text digital content rendering module element. Accordingly Applicants respectfully submit that Claims 2-17 and 29-33 are allowable at least by similar reasoning.

Claim 18 recites an apparatus comprising, *inter alia*,

> a plurality of digital content rendering modules communicatively coupled with each other in a hierarchical manner forming a hierarchy of modules, with selective combinations of the modules to be selectively employed to protectively render digital content of various types, including one of said digital content rendering modules occupying a root position of the hierarchy to exclusively receive the various types of digital contents to be rendered, **from a recovery module not part of the hierarchy of modules, the recovery module being responsible for recovering the digital contents from their ciphered states**, the recovery module employing measures to hinder observation of operations performed therein, and the root modules

being operative for verifying a module occupying an immediate downstream position in the hierarchy of modules from the root module as not having been compromised....

Applicants respectfully submit that *England* does not teach or suggest a root digital content rendering module "to exclusively receive the various types of digital contents to be rendered, **from a recovery module not part of the hierarchy of modules**." On the contrary, at col. 3 lines 14-18, *England* specifically states, "[s]ecure pages **handle premium content with a system of code modules in a hierarchy of trust**, where a module names other modules that it is willing to trust, and those modules in turn name other modules that they are willing to trust." At most, *England* may disclose merely that a content provider at the low end of the trust hierarchy may be able to decrypt data. Applicants respectfully submit that in no case does *England* teach or even suggest that a root digital content rendering module may exclusively receive digital content from a recovery module that is **not part of the hierarchy of modules** and that is **responsible for recovering the digital contents from their ciphered states**, as claimed in Claim 18. Applicants can discern no teaching or suggestion in *Graunke* that remedies this defect. Accordingly, Applicants respectfully submit that Claim 18 is not obvious considering *England* in view of *Granke*. Claims 19-24 depend from Claim 18 and are allowable at least by dependency.

CONCLUSION

For at least the reasons above, Applicants respectfully submit that Claims 1-33 are allowable and request that the Examiner permit these claims to proceed to issuance. Although additional arguments are believed to exist for the allow ability of the claims (for example, that one of ordinary skill in the art would have had no motivation to make the asserted combination of references), the arguments presented are believed sufficient to address the Examiner's rejections. Likewise, failure of the Applicants to respond to a position taken by the Examiner is not an indication of acceptance or acquiescence of the Examiner's position. Instead, it is believed that the Examiner's positions are rendered moot by the foregoing arguments and amendments, and it is therefore not believed necessary to respond to every position taken by the Examiner with which Applicants do not agree.

The Examiner is respectfully requested to contact the undersigned at the telephone number below if there are any remaining questions regarding this application.

We believe the appropriate fees accompany this transmission. If, however, insufficient fee payment or fee overpayment occurs, the amount may be withdrawn or deposited from/to AXIOS Law Group's deposit account. The deposit account number is 50-4051.

Respectfully submitted,

AXIOS LAW GROUP

Date: October 27, 2008

by: /Adam L.K. Philipp/
Adam L.K. Philipp
Reg. No.: 42,071

AXIOS Law Group
1525 4th Avenue N, Suite 800
Seattle, WA 98101
Telephone: 206-217-2200